UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF: **THE OATH, INC. ACCOUNT ASSOCIATED WITH GFORBIDDENG@VERIZON.NET**	**CASE NO.** 1:21-mj-2478 TMD

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Christine D. Carlson, being duly sworn, depose and state that:

1. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI), assigned to the Special Agent in Charge in Baltimore, Maryland. I have been so employed since June 1996. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, transportation, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of search warrants, which involved child exploitation and/or child pornography offenses. I am currently assigned to the Maryland State Police Internet Crimes Against Children Task Force (ICAC) which is comprised of federal, state and local law enforcement working jointly to combat child exploitation in the State of Maryland.

2. I have received formal training from U.S. Customs and HSI and other agencies in the area of child pornography, pedophile behavior, collectors of other obscene material and Internet crime. This includes, but is not limited to, use of Internet facilities to produce child pornography in violation of 18 U.S.C. § 2251(a), and possess child pornography in violation of 18

U.S.C. § 2252A(a)(5)(B).

3. As a federal agent, I am authorized to investigate violations of laws of the United States and is a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

4. This affidavit is made in support of an application for a warrant to search the following (hereinafter referred to as the "TARGET ACCOUNT"):

a. The Oath, Inc. account associated with the email address **gforbiddeng@verizon.net** maintained by Oath, Inc., 22000 AOL Way, Dulles, VA 20166.

5. The TARGET ACCOUNT is to be searched for evidence of violations of Title 18, United States Code, Section 2251(a) (production of child pornography) and Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography) (hereinafter referred to as the "TARGET OFFENSES").

6. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of violations of the aforementioned federal statutes are located in the TARGET ACCOUNT.

7. The information contained in this affidavit came from my own participation in the inquiry described herein, as well as documents and reports prepared by other law enforcement officers, including the Maryland State Police and other third parties, and in each instance, I have identified the source of information upon which I have relied.

SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY

8. Based upon my experience in child exploitation investigations and upon

information provided me by other law enforcement officers, the following can be true of child molesters/child pornographers:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms,

have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

9. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

d. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo!, Google, Inc., Facebook, Dropbox, and Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including e-mail, images, videos, and other files. The data is maintained on the servers of the providers and is occasionally retained by the providers after the user deletes the data from their account.

f. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

10. Based on traits shared by collectors, the use of e-mail, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the production, receipt and possession of child pornography will be found in the TARGET ACCOUNT, notwithstanding the passage of time.

PROBABLE CAUSE

11. On September 11, 2017, a Harford County Sheriff's Deputy responded to Walgreens, located at 1927 Emmorton Road, Bel Air, Maryland 21014. The sheriff's deputy arrived and spoke to a Walgreens photo clerk who had observed inappropriate photographs of children on a customer's phone while assisting the customer with locating and saving photos to be printed from the customer's cell phone. The Walgreens employee stated the individual had uploaded approximately 300-400 photos onto the Walgreens photo kiosk. While assisting the customer with printing images, the Walgreens employee observed images of two young children, a boy, and a girl, naked with bruises and bite marks on their bodies. The employee also observed

images that showed the boy's and girl's "butts." The employee also observed nude images of the customer, however, did not see images of the customer nude with the children. The Walgreens employee identified the customer as Fernando Cristancho ("CRISTANCHO"). The Walgreens employee provided the responding sheriff's deputy with pictures of the two children as well as a picture identified as the customer, CRISTANCHO.

12. On September 18, 2017, Master Trooper First Class Adam LeCompte, assigned to the Harford County Internet Crimes Against Children Task Force/Child Advocacy Center contacted the Walgreens employee who was able to re-affirm the descriptions of the photos. The Walgreens employee believed the images depicted human bites on the buttocks of the minor male child and that this minor was approximately 4 years old. The Walgreens employee believed the minor female was approximately 6 years old. The Walgreens employee remembered the images depicted the minor female with bruises and bite marks and with her underwear soaking wet.

13. On September 19, 2017, the Harford County Internet Crimes Against Children Task Force executed a state search warrant at CRISTANCHO's residence, located at 811 Hayden Way, Bel Air, Maryland 21014. During the execution of the state search warrant numerous computer devices were located and seized. During the execution of the search warrant, CRISTANCHO arrived at his residence. CRISTANCHO was in possession of an iPhone 6s which he turned over to investigators executing the search warrant. Maryland State Police Master Trooper Adam LeCompte conducted a preview of this cell phone and discovered numerous images in the Google Photos folder of the cell phone including several images of a prepubescent minor male. The minor male has been identified and will be referred to as K.C., who was 2-3 years old at the time of the photo. The images are all dated "Saturday, July 4, 2015." The first image depicts Minor Victim K.C. from the chest up, nude, leaning against a wall mirror. His reflection in the mirror also

appears in the image. The second image also depicts K.C. leaning against a wall mirror. Minor Victim K.C. is nude and his reflection is fully visible in the image and his genitals are exposed in the reflection. The third image depicts K.C., nude, holding his genitals in the image. K.C.'s midsection and genitals are visible in the image. In addition, there are two other images of K.C. that depict the minor wearing a t-shirt or towel wrapped around his forehead. Only K.C.'s face and head are visible in these images.

14. On February 1, 2018, HSI Special Agent Augustus Aquino applied for and obtained a federal search warrant issued by the Honorable U.S. Magistrate Judge Beth P. Gesner to search the digital devices, including the Apple iPhone 6s seized from CRISTANCHO's residence. An examination of this cell phone revealed numerous images of K.C. with his genitals exposed. In addition, the information attached to the images indicates the photos were taken using an iPhone 5s and iPhone 6s in 2015 through 2017. By way of example, a description of one of these images is as follows:

> **IMG_0022.JPG** – depicts K.C. standing on a table, the image is a close-up of the victim's genitals and only the midsection and genitals are visible. This image is a part of a series of images contained in the iPhone 6s that depicts K.C. standing on a table and in the background the kitchen of the residence is visible.

The "metadata" for the image indicates it was taken using an iPhone 5s on March 10, 2015, when K.C. was 2-3 years old.

15. During the examination of the iPhone 6s seized from CRISTANCHO, I also observed several videos stored on this cell phone. By way of example, a description of the video is as follows:

> **IMG_3682.MOV** – depicts a nude minor male (believed to be K.C.) sitting on a toilet with legs spread to expose his genitals in the video. The video is only several seconds in length but at the end of the video a hand reaches into the video and grabs the minor's genitals.

The metadata identifies the video was taken with an iPhone 6s on August 3, 2017. In addition, the video contains location data indicating the file was produced at CRISTANCHO's residence located at 811 Hayden Way, Bel Air, Maryland 21014.

16. On February 21, 2018, CRISTANCHO was indicted by a federal Grand Jury in the District of Maryland and charged with one count of Production of Child Pornography, in violation of 18 U.S.C. § 2251(a). The single count indictment related to the video and associated files described in paragraph 15 above.

17. In addition to the files described above, the examination of CRISTANCHO's phone and other digital storage devices found in his residence during the search warrant on September 19, 2017, the following images were located:

a. A series of 8 images of a female infant created on January 18, 2012. The female has been identified and will be referred to as C.C. The images appear to be taken following and bath, and the first 6 images depict C.C. wrapped in a hooded towel, in her mother's arms, and both of them are facing the camera. The seventh image depicts C.C.'s exposed buttocks, and the 8th image is a close-up image of C.C.'s inner thighs and exposed genitals;

b. A series of 15 images created in December 2012, that depict CRISTANCHO, an adult female, a minor male and a minor female. The minor male has been identified and will be referred to as J.C., and the minor female has been identified and will be referred to as H.C. Both were 11 years old in December 2012. The series of photos starts with CRISTANCHO, the adult female and J.C. on the couch, with J.C. wearing only shorts. As the series continues, all three are still on the couch, and J.C. is nude, with his arms and legs spread wide apart, exposing his genitals. Two images depict J.C. standing, nude, and in one of these, his hands are on his inner thighs and his legs are spread, exposing his genitals. The next image is a close up of J.C.'s midsection, J.C. is wearing underwear, and he is pulling his underwear away from his body to expose his genitals, which are the focal point of the image. Another image depicts H.C. from behind, with her pants at her knees, exposing her buttocks. The next image depicts H.C., from the front, standing with her arms spread out to her side and her pants pulled down to her knees, and her genitals exposed.

18. The examination of the cell phone indicated the Apple ID for the cell phone is fdocristancho@gmail.com and lists the name of the cell phone as "Fernando's iPhone". The telephone number associated with the iPhone 6s is listed as "410 937-1178." Additionally, the

phone contained emails to/from the email accounts fdocristancho@gmail.com and **gforbiddeng@verizon.net**. Several logins to Verizon webmail were also located in the web history on the iPhone.

19. On April 2, 2019, a search warrant was authorized for the Apple account associated with the email address fdocristancho@gmail.com and the email account fdocristancho@gmail.com.

20. The search warrants were served on Apple, Inc. and Google, Inc. via email or law enforcement portal along with their respective attachments.

21. A review of the Google search warrant return for the email account fdcristancho@gmail.com revealed the recovery email for the account as **gforbiddeng@verizon.net**. Additionally, there were several emails to the email account **gforbiddeng@verizon.net** or where the email account **gforbiddeng@verizon.net** was copied on an email contained within the email account fdcristancho@gmail.com. There were also searches conducted within the Google account for "fucking teens," "two young boys having sex," and "show me a dick masturbation" as well as web history searches for photos of boys having sex with each other, how to masturbate if you're a real boy and school boy masturbating himself and cums.

22. A summons was issued to Oath, Inc., for the email account **gforbiddeng@verizon.net**. Oath, Inc. responded and provided the following subscriber information:

Mail Name:	gforbiddeng@verizon.net
Account Status:	active
Registration Date:	2017-02-07T11:31:12.000Z
Full Name:	Fernando Cristancho
Country:	US
Zip/Postal Code:	21014
Recovery Phones:	+14109371138 Unverified +14109371178 Verified

23. On June 23, 2021, CRISTANCHO was indicted by a federal Grand Jury in the District of Maryland in a second superseding indictment and charged with one count of Coercion and Enticement of a Minor, in violation of 18 U.S.C. § 2422(b), six counts of Production of Child Pornography, in violation of 18 U.S.C. § 2251(a), and three counts of Possession of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B).

DSS INVESTIGATIONS

24. During the course of my investigation, through the review of records from the Maryland Department of Social Services and the Harford County Child Abuse Center, I have learned about two investigations into CRISTANCHO.

2006 CAC Investigation of CRISTANCHO:

25. In 2006 the CAC conducted an investigation into allegations that CRISTANCHO sexually abused his two biological sons, both age 5 at the time (one of these is J.C., referenced above). The investigation determined that CRISTANCHO was "indicated" for sexually abusing his sons. The term indicated means that there is credible evidence which has not been satisfactorily refuted. No criminal charges were filed as a result of the investigation.

2017 CAC Investigation of CRISTANCHO:

26. On September 14, 2017, Harford County DSS received a referral of new allegations of sexual abuse and neglect by CRISTANCHO, relating to his biological children, K.C. (4) and C.C (6). The allegation was that CRISTANCHO slept in a locked bedroom alone with his son K.C., age 4, and that K.C.'s mother does not have access to the room.

REQUEST TO EXECUTE WARRANT AT ANY TIME

27. Because the warrant on the TARGET ACCOUNT will be served on Oath, Inc., which will then compile the requested records at a time convenient to each, reasonable cause exists

to permit the execution of the requested warrant at any time in the day or night.

SUMMARY

28. Based on my training and experience, as well as the images described above that were located on CRISTANCHO's devices, I believe that CRISTANCHO has a sexual interest in children and displays characteristics common to individuals who access with the intent to view and/or, possess, collect, receive, or distribute child pornography as discussed in paragraphs 8 and 9 above. Based on these characteristics and because the TARGET ACCOUNT appears to be accessed, controlled and/or created by CRISTANCHO, I respectfully submit there is probable cause that the TARGET ACCOUNT contains evidence (1) of production and/or possession of child pornography, and (2) are relevant to determine the ownership and control of the accounts that are linked to the production, receipt, and possession of child pornography. Based on my training and experience, such information may constitute evidence of the TARGET OFFENSES because the information can be used to identify the account's user or users.

CONCLUSION

29. Based on the foregoing information, I have probable cause to believe that contraband, and evidence, fruits, and instrumentalities of violations of the TARGET OFFENSES as set forth herein and in Attachment B, are currently contained in the TARGET ACCOUNT more fully described in Attachment A. I therefore respectfully request that a search warrant be issued authorizing a search of the TARGET ACCOUNT for the items described above and in Attachment B and authorizing the seizure and examination of any such items found therein.

30. Pursuant to Title 18 U.S.C. 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

CHRISTINE D CARLSON Digitally signed by CHRISTINE D CARLSON

Special Agent Christine D. Carlson
Homeland Security Investigations

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. and 41(d)(3) on this 31 day of August, 2021.

HONORABLE THOMAS D. DIGIROLAMO
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
(Oath, Inc.)

This warrant applies to information associated with the following Oath Inc. account:

- **gforbiddeng@verizon.net**;

which is stored at the premise owned, maintained, controlled, or operated by Oath, Inc., with offices located at 22000 AOL Way, Dulles, VA 20166.

ATTACHMENT B
(Oath, Inc.)

I. Files and Accounts to be produced by Oath Inc. between February 7, 2017, to the present.

Oath, Inc. shall disclose responsive data, if any by sending to Homeland Security Investigations, 40 South Gay Street, Third Floor, Baltimore, MD 21202, ATTN: Special Agent Christine Carlson, or christine.d.carlson@ice.dhs.gov, using UPS or another courier service or email, notwithstanding 18 U.S.C. § 2252A or similar statute or code.

To the extent that the information described in Attachment A is within the possession, custody, or control of Oath, Inc. including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Oath, Inc., Oath, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails, attachments, and chat messages stored in the account described in Attachment A, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All existing printouts from original storage of all of the electronic mail described above in Section I.A. above;

c. All internet search data including all queries and location data;

d. All transactional information of all activity of the electronic mail address described above in Section I.A., including log files, dates, times, methods of connecting, ports, dial ups, and/or locations;

e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

f. All records or other information regarding the identification of the account described above in Section I.A., to include application, full name, physical address, telephone numbers, and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all screen names associated with subscribers and/or accounts, all account names associated with the subscriber, methods of connecting, log files, means and source of payment (including any credit or bank account number), and detailed billing records;

g. All records indicating the services available to subscribers of the electronic mail address described above in Section I.A.;

h. AIM conversation logs and files shared associated with the accounts listed in Attachment A;

i. Payment information, including billing address, shipping address, and payment instruments, associated with any AOL or Oath, Inc. services used by the account listed in Attachment A.

II. Information to be Seized by Law Enforcement Personnel

a. Any and all records that relate in any way to the account described in Attachment A which is evidence, fruits, and instrumentalities of violations of Title 18 U.S.C.§§ 2251(a) and 2252A(a)(5)(B), specifically that relate to the following:

1. Images, videos and other files depicting the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

2. Communications or documentations regarding the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

3. Communication or documentation regarding access to and/or interaction with minors, to include the enticement of a minor;

4. Images depicting the interior or exterior of residences, public establishments, and vehicles;

5. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;

6. Communication, information, documentation and records relating to who created, used, controlled or communicated with the account or identifier, including records about their identities and whereabouts;

7. Evidence of the times the account or identifier listed on Attachment A1 was used;

8. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

9. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A1 and other associated accounts;

10. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

b. All existing printouts from original storage which concern the categories identified in subsection II.A; and

c. All “address books” or other lists;

With respect to the search of the information provided pursuant to this warrant by the above-referenced provider, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If after performing these procedures, the directories, files, or storage areas do not reveal evidence of child pornography or other criminal activity, the further search of that particular directory, file or storage area, shall cease.

If the government identified any seized communication that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.